ABSTRACT
For
AUTHENTICATION IN A TELECOMMUNICATIONS NETWORK

The invention relates to an authentication method intended for a telecommunications network, especially for an IP network. From a terminal (TE1) in the network a first message (RR) containing an authenticator and a data unit is transmitted to the network, the data unit containing information relating to the manner in which the authenticator is formed. For carrying out authentication in the network, the data unit contained in the first message is used for determining a check value, which is compared with the said authenticator. To make it unnecessary for the terminal to perform any complicated and heavy exchange of messages when attaching to the network and for still obtaining the desired security characteristics for use, such an identification unit is used in the terminal which receives as input a challenge from which a response and a key can be determined essentially in the same manner as in the subscriber identity module of a known mobile communications system, a set of authentication blocks is generated into the network, of which each contains a challenge, a response, and a key, whereby the generation is performed in the same manner as in the said mobile communication system, at least some of the challenges contained by the authentication blocks are transmitted to the terminal, one of the challenges is chosen for use at the terminal, and, based on it, a response and key for use are determined with the aid of the terminal's identification unit, in the said first message (RR) the network is notified with the aid of the said data unit of which key corresponding to which challenge was chosen, and the authenticator of the first message and the said check value are determined with the aid of the chosen key.